PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-205738

(43)Date of publication of application : 30.07.1999

---

(51)Int.Cl. H04N 5/92

H04L 9/10

H04N 5/907

---

(21)Application number : 10-003367 (71)Applicant : CANON INC

(22)Date of filing : 09.01.1998 (72)Inventor : OISHI KAZUOMI

---

(54) IMAGE INPUT DEVICE, ITS METHOD AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To maintain high security independently of a tamper resistance of an information input device.

SOLUTION: The device 100 is provided with a conversion means 102 that converts an image signal into digital information, an encryption means 104 that encrypts the digital information, an encryption key entry means 109 that enters externally an encryption key by which the encryption means 104 conducts encryption, and an encryption key delete means 105 that deletes the encryption key after the encryption means 104 finishes encryption of the digital information. Thus, encryption key (decoding key) to decode the encrypted information cannot be obtained by a third party.

LEGAL STATUS [Date of request for examination] 07.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The picture input device characterized by having a conversion means to change a picture signal into digital information, an encryption means to encipher said digital information using an encryption key, and an encryption key elimination means to eliminate said encryption key after said encryption means completes encryption of said digital information.

[Claim 2] It is the picture input device according to claim 1 which said conversion means has the coding means which carries out high efficiency coding of said digital information, and is characterized by said encryption means enciphering said digital information which carried out high efficiency coding.

[Claim 3] It is the picture input device according to claim 1 or 2 which has an image pick-up means to photo a photographic subject and to generate a picture signal, and is characterized by said conversion means changing into digital information the picture signal generated by said image pick-up means.

[Claim 4] A picture input device given in any 1 term of claims 1-3 characterized by providing an encryption key input means to input said encryption key from the outside.

[Claim 5] A picture input device given in any 1 term of claims 1-3 characterized by providing an encryption key generating means to generate said encryption key inside.

[Claim 6] Said encryption key is a picture input device according to claim 4 or 5 characterized by being an encryption key for common-key-encryptosystem-izing.

[Claim 7] The picture input device according to claim 5 characterized by outputting the internal encryption key which possessed the interface which inputs from the outside the internal encryption key generated with said encryption key generating means, and was enciphered through said interface.

[Claim 8] It is the picture input device according to claim 7 which said internal encryption key is an encryption key for common-key-encryptosystem-izing, and is characterized by said external encryption key being an encryption key for public-key-encryption-izing.

[Claim 9] A picture input device given in any 1 term of claims 1-8 characterized by providing the means of communications which outputs said enciphered digital information outside.

[Claim 10] A picture input device given in any 1 term of claims 1-9 characterized by providing a record means to record said enciphered digital information.

[Claim 11] The image input approach characterized by performing transform processing which changes a picture signal into digital information, encryption

processing which enciphers said digital information using an encryption key, and encryption key elimination processing which eliminates said encryption key after completing encryption of said digital information.

[Claim 12] The image input approach according to claim 11 which carries out high efficiency coding of said digital information, and is characterized by enciphering said digital information by which high efficiency coding was carried out.

[Claim 13] The image input approach according to claim 11 or 12 characterized by generating said picture signal by image pick-up processing which photos a photographic subject.

[Claim 14] The image input approach given in any 1 term of claims 11-13 characterized by performing output processing which outputs said enciphered digital information outside.

[Claim 15] The image input approach given in any 1 term of claims 11-14 characterized by performing record processing which records said enciphered digital information.

[Claim 16] The storage characterized by storing the program for operating a computer as each means according to claim 1 to 10.

[Claim 17] The storage characterized by storing the program for making a computer perform the procedure of the image input approach of a publication in

any 1 term of claims 11-15.

[Claim 18] The picture input device characterized by having a conversion means to change a picture signal into digital information, an encryption means to encipher said digital information, and an encryption key input means to input an encryption key for said encryption means to encipher from the outside.

[Claim 19] The storage characterized by memorizing the key for decoding said digital information as which it can detach and attach freely to the picture input device which has a conversion means to change a picture signal into digital information, and an encryption means to encipher said digital information, and said encryption means enciphers it, and which was sake [digital information] and enciphered.

[Claim 20] The picture input device characterized by having a conversion means to change a picture signal into digital information, an image encryption means to encipher said digital information with an internal encryption key, a key encryption means to encipher said internal encryption key, and an encryption key input means to input an encryption key for said key encryption means to encipher from the outside.

[Claim 21] The storage characterized by to memorize the decode key for decoding an encryption key and said internal encryption key which were enciphered being able to detach and attach freely to the picture input device

which has a conversion means change a picture signal into digital information, an image encryption means encipher said digital information with an internal encryption key, and a key encryption means encipher said internal encryption key, and said key encryption means enciphering.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a storage at a picture input device and an approach list.

[0002]

[Description of the Prior Art] Picture input devices, such as a still camera, a video camera, or a scanner, input the picture signal of a picture signal, a dynamic image, a static image, etc. which photoed the photographic subject and were obtained, and he changes and outputs it to the format which can be reproduced as image information, or is trying to record it on a storage using a recording

device.

[0003] Since said storage can be saved over a certain amount of long period of time, it is convenient for admiring said saved image information later, or reusing it. Moreover, a regenerative apparatus forms an image significant to **** from the image information recorded on said storage, and reproduces an image using output units, such as a printer and a display.

[0004] Recently, said picture input device realized with the analog form is being conventionally switched gradually to the thing of a digital method by progress of a digital technique. After in almost all cases the picture input device of these digital methods catches the candidate for photography for an input optically, carries out photo electric conversion of it, generates an electrical signal and subsequently carries out an analog / digital conversion, it is made to perform a predetermined image processing. And it outputs as digital information of the format that the image/image information formed as the result were able to be defined beforehand.

[0005] Here, the format defined beforehand means the thing of the sign by the information source coding method to an image/image information, such as MH, MR, MMR, TIFF, and JPEG, MPEG.

[0006] And when a regenerative apparatus outputs the information decoded and formed from the sign by using the decode algorithm to output units, such as a

printer and a display, it is the information which human being can understand as an image/an image.

[0007] Below, the image/image information outputted as digital information of the above-mentioned format defined beforehand are called the image/image information by which information source coding was carried out. It is very easy to incorporate the image / image information by which information source coding was carried out, or the image/image information decoded from it to an information processor like a personal computer, and to edit it using the image / image information edit processing software corresponding to the format.

[0008] The image quality when reproducing the image / image information by which information source coding was carried out, or the information which edited it is completely the same as that of the original. In the case of the conventional analog form, although the limit was imposed on the image processing since edit and a duplicate had surely brought about degradation of image quality, the digital method brought about improvement in overwhelming convenience at this point.

[0009] By the way, repeating a duplicate in the conventional analog form had that it posed [little] a big problem actually, even if it might say that an illegal duplicate action was performed although surely accompanied by degradation of image quality therefore. Therefore, especially the method of forbidding such an

unjust duplicate action was not established.

[0010] However, since it is possible to generate the completely same duplicate as the original to ****** by the digital method, if anyone can perform a duplicate action freely, since the need that a consumer pays the countervalue to the admiration right of a work to the manufacturer of image works, such as a movie, etc. is lost, it is clear to become a big threat to the manufacturer of a work etc.

[0011] Or when the image/image information used as the original of a work are recorded on the computer as another example as image information by which information source coding was carried out, a cracker accessing the computer, reproducing its image/image information unfairly, and selling at a price cheaper than the work product of normal or newly editing the work and selling as other works are also considered.

[0012] The cure using the technique of the code described below to the problem of the above duplicates of digital information is effective. In addition, a code means changing information so that informational semantics may not be understood those days other than a person.

[0013] In a code, the original sentence is called plaintext. Moreover, it is called encryption to change into the cipher as which a third person does not understand semantics for it, and the conversion procedure is called cryptographic algorithm. Even if it calls it a plaintext and a cipher, it does not

necessarily restrict to a text, and all information, such as data, voice, and an image, is assumed.

[0014] Encryption is conversion depending on a parameter called an encryption key. It is called decode that a person concerned returns a cipher to the original plaintext, and it is performed using the parameter (it is called a decode key) corresponding to an encryption key.

[0015] Moreover, it is called decode that third persons other than a person concerned return a cipher to the original plaintext or to find out a decode key. If it is made to come back to the key which uses the safety of a code for a code or decode and a key is not known, even if it knows cryptographic algorithm, the plaintext is made from the present-day code so that it may not be obtained. Therefore, the implementer of a code machine cannot do decode, either.

[0016] Although there are many algorithms in a code, it classifies into two, an unsymmetrical code (public key encryption) and a symmetrical code (common use code), according to below from a viewpoint of whether to be able to exhibit an encryption key.

[0017] It is also called public key encryption and an encryption key differs from a decode key, a decode key can calculate an unsymmetrical code no longer easily from an encryption key, it calls an encryption key a public key, and says the thing of the code used for a decode key, holding secretly.

[0018] The unsymmetrical code has the following descriptions.

(1) Since an encryption key differs from a decode key and an encryption key can be exhibited, it is not necessary to deliver an encryption key secretly, and key delivery is easy.

(2) Since each user's encryption key is exhibited, the user should memorize only each one of decode keys in secret.

(3) An authentication function for an addressee to check that the transmitting person of the sent correspondence is not imitation and that the correspondence is not altered is realizable. As an unsymmetrical code which can realize a code function and an authentication function, there is RSA cryptograph (R. L.Rivest, A.Shamir and L.Adleman, and "A method ofobtaining digital signatures and public key cryptosytems" Comm of ACM).

[0019] Moreover, in addition to this, an ElGamal cryptosystem (472 31 T. E.ElGamal, "A public key cryptosystem and a signaturescheme based - discretre logarithms", IEEE Transaction on Information Theory, Vol.IT- No. 4, pp-469-1985) is famous.

[0020] As an unsymmetrical code which can realize only an authentication function Fiat-Shamir code (A.) [Fiat, A.Shamir,] ["How to prove yourself:practical solutions of idcntification and] signature problems, ", and Proc.of CRYPTO' -- 86 and 1987 -- A Schnorr code (C. P.Schnorr, "Emcient

signature generationby smart cards, "Journal of Cryptolgyvol 4, pp.161-174, and 1991) are famous.

[0021] An encryption key and a decode key are the same codes, and the symmetry code is also called the common key encryptosystem. Public key encryption appears late in the 1979s, and the symmetry code which exists from the former also came to be called a common use code.

[0022] A symmetry code can be divided into the block cipher enciphered with the same key to every [of suitable die length] character string (block), and the stream cipher which changes the key for every character string or bit.

[0023] There are a transposition cipher which replaces the sequence of an alphabetic character and is enciphered, a substitution type code which changes an alphabetic character to other alphabetic characters in a block cipher, and DES (Data Encryption Standard) to which the algorithm is opened, and a code called FEAL (Fastdata Encipherment ALgorithm) are widely used as a commercial code.

[0024] Stream cipher is a method which carries out XOR (exclusive OR) of the random number to a message, and carries out disturbance of the contents, and is famous for the Barnum code using the random number sequence of an infinity period as a disposable key only for 1 time.

[0025] If it enciphers to the image/image information recorded on a computer etc.

using the technique of the above code and the decode key is kept safely, even if the information which enciphered the cipher, i.e., an image/image information, will be stolen and reproduced, since it does not mean that the image / the image information itself were stolen, it does not suffer damage. That is, it is thought that the problem of the above duplicates is solvable.

[0026] However, since encryption was performed on the computer after an image/image information was conventionally outputted to the computer etc., it existed as the image/image information by which information source coding was carried out after an image/image information is outputted from a picture input device until it was enciphered on the computer, and there was a problem that an image/image information will be stolen in the meantime.

[0027] There is the coping-with method which enciphers inside a picture input device to this problem. At this time, it is necessary to incorporate encryption **** so that an image/image information before being enciphered may not be taken out outside.

[0028] A sensor forms in forming the encryption section into IC chip, and the interior of the encryption section which formed into IC chip further so that it may become difficult physically to take out the program stored in the interior and data as such a means, and when the physical actuation which is going to take out the data inside IC chip detects, the thing of eliminating and destroying the program

and the data of the interior can consider. The resistance over the attack from such the outside is called tamper resistance (Tamper Resistance).

[0029]

[Problem(s) to be Solved by the Invention] In the picture input device incorporating the encryption section which has tamper resistance, in order not to weaken the reinforcement, the value of immobilization is beforehand recorded on equipment as an encryption key, and, as for the value, it is common that it cannot change easily.

[0030] when one key is assigned to one equipment, and two or more users share and use it, there is no encryption (secrecy) function among those users --- alike and equal.

[0031] Although there is also a method of preparing two or more keys beforehand and on the other hand using a separate key for every user, the amount of memory of the encryption section inside equipment increases at this time, and the problem which leads to the rise of cost arises.

[0032] Anyway, there was a problem that it could not respond according to an individual to many and unspecified users. Furthermore, equipment or the medium which have these tamper resistances did not restrict having the property forever, but also had a possibility that the property might be easily cancelled by the new attack means.

[0033] This invention aims at enabling it to maintain safety in view of the above-mentioned trouble, without being dependent on the tamper resistance of an information input device.

[0034]

[Means for Solving the Problem] The picture input device of this invention is characterized by having a conversion means to change a picture signal into digital information, an encryption means to encipher said digital information using an encryption key, and an encryption key elimination means to eliminate said encryption key after said encryption means completes encryption of said digital information.

[0035] Moreover, in the place by which it is characterized [of the picture input device of this invention / other], said conversion means has the coding means which carries out high efficiency coding of said digital information, and it is characterized by said encryption means enciphering said digital information which carried out high efficiency coding.

[0036] Moreover, it has an image pick-up means for the place by which it is characterized [of others of the picture input device of this invention] to photo a photographic subject, and to generate a picture signal, and said conversion means is characterized by changing into digital information the picture signal generated by said image pick-up means.

[0037] Moreover, the place by which it is characterized [of others of the picture input device of this invention] is characterized by providing an encryption key input means to input said encryption key from the outside.

[0038] Moreover, the place by which it is characterized [of others of the picture input device of this invention] is characterized by providing an encryption key generating means to generate said encryption key inside.

[0039] Moreover, the place by which it is characterized [of others of the picture input device of this invention] is characterized by said encryption key being an encryption key for common-key-encryptosystem-izing.

[0040] Moreover, the place by which it is characterized [of others of the picture input device of this invention] possesses the interface which inputs from the outside the internal encryption key generated with said encryption key generating means, and is characterized by outputting the internal encryption key enciphered through said interface.

[0041] Moreover, it is characterized by for said internal encryption key being an encryption key for common-key-encryptosystem-izing the place by which it is characterized [of others of the picture input device of this invention], and said external encryption key being an encryption key for public-key-encryption-izing.

[0042] Moreover, the place by which it is characterized [of others of the picture input device of this invention] is characterized by providing the means of

communications which outputs said enciphered digital information outside.

[0043] Moreover, the place by which it is characterized [of others of the picture input device of this invention] is characterized by providing a record means to record said enciphered digital information.

[0044] The image input approach of this invention is characterized by performing transform processing which changes a picture signal into digital information, encryption processing which enciphers said digital information using an encryption key, and encryption key elimination processing which eliminates said encryption key after completing encryption of said digital information.

[0045] Moreover, the place by which it is characterized [of the image input approach of this invention / other] carries out high efficiency coding of said digital information, and is characterized by enciphering said digital information by which high efficiency coding was carried out.

[0046] Moreover, the place by which it is characterized [of others of the image input approach of this invention] is characterized by generating said picture signal by image pick-up processing which photos a photographic subject.

[0047] Moreover, the place by which it is characterized [of others of the image input approach of this invention] is characterized by performing output processing which outputs said enciphered digital information outside.

[0048] Moreover, the place by which it is characterized [of others of the image

input approach of this invention] is characterized by performing record processing which records said enciphered digital information.

[0049] Moreover, the storage of this invention is characterized by storing the program for operating a computer as said each means.

[0050] Moreover, the place by which it is characterized [of the storage of this invention / other] is characterized by storing the program for making a computer perform the procedure of said image input approach.

[0051] Moreover, the place by which it is characterized [of others of the picture input device of this invention] is characterized by having a conversion means to change a picture signal into digital information, an encryption means to encipher said digital information, and an encryption key input means to input an encryption key for said encryption means to encipher from the outside.

[0052] Moreover, the place by which it is characterized [of others of the storage of this invention] can be freely detached and attached to the picture input device which has a conversion means to change a picture signal into digital information, and an encryption means to encipher said digital information, and is characterized by memorizing the key for decoding said digital information as which said encryption means enciphers it and which was sake [digital information] and enciphered.

[0053] Moreover, the place by which it is characterized [of others of the picture

input device of this invention] is characterized by to have a conversion means change a picture signal into digital information, an image encryption means encipher said digital information with an internal encryption key, a key encryption means encipher said internal encryption key, and an encryption key input means input an encryption key for said key encryption means to encipher from the outside.

[0054] Moreover, the place by which it is characterized [of others of the storage of this invention] A conversion means to change a picture signal into digital information, and an image encryption means to encipher said digital information with an internal encryption key, It can detach and attach freely to the picture input device which has a key encryption means to encipher said internal encryption key, and is characterized by memorizing the decode key for decoding an encryption key and said enciphered internal encryption key for said key encryption means enciphering.

[0055] Since this invention consists of said technical means, an encryption key is eliminated from an information input unit after encryption termination, and it becomes possible to maintain safety, without it becoming impossible for a third person to get an encryption key (decode key) for this to decode the enciphered information, and being dependent on the tamper resistance of an information input unit.

[0056] Moreover, since an encryption key (decode key) is inputted using an interface with the exterior, while according to other descriptions of this invention being able to respond to many and unspecified users and being able to save the time and effort of actuation of human being, an encryption key can lessen a possibility that it may be stolen by the third person.

[0057]

[Embodiment of the Invention] (Gestalt of the 1st operation) Next, the gestalt of operation of the 1st of a storage in the picture input device and approach list of this invention is explained to reference for drawing 1 .

[0058] Drawing 1 is the block diagram showing the outline of the picture input device of the gestalt of this operation, for image pick-up equipment and 2, as for the memory for control programs, and 4, a central information processor (CPU) and 3 are [1 / working-level month memory and 5] encryption machines, and it is shown that this serves as the module 10 by which closure unification was carried out so that it might have tamper resistance.

[0059] In the picture input device of the gestalt of this operation, the object to read is picturized with image pick-up equipment 1, the picture signal of an analog is generated, and it is made to perform digital transform processing which changes this into a digital image signal.

[0060] Said image pick-up equipment 1 is controlled so that a good image is

obtained by the program stored in the memory 3 for control programs, and it operates so that image data may be outputted as the result.

[0061] Next, after an image processing etc. is performed to this image data in CPU2, it is changed into the image/image information by which information source coding (high efficiency coding) was carried out, and is inputted into the encryption machine 5. By making into a parameter the encryption key inputted from an external interface 7, the encryption machine 5 performs encryption to an input in the interior, and generates and outputs a cipher. The outputted image data which was enciphered is memorized by the non-illustrated storage. An external interface 7 is an interface which receives an encryption key from the equipment exterior, or is used since an encryption key is outputted from the inside of equipment.

[0062] In the aforementioned configuration, data or the contents of a communication link which exist in image pick-up equipment 1, CPU2, the memory 3 for control programs, the working-level month memory 4, and the interior of the encryption machine 5 cannot be acquired from the exterior according to the description of tamper resistance.

[0063] Next, the combination of the specification method of the cipher system and encryption key which are used for encryption is explained. The cipher system to be used has two cases, public key encryption and a common key

encryptosystem. To use a common key encryptosystem, it is necessary to specify an encryption key not known by the others. On the other hand, when using public key encryption, it is not necessary to specify that it is not necessarily known by the others since an encryption key can be exhibited.

[0064] The specification method of an encryption key has the following approaches. That is, the 1st approach is an approach which the memory 3 for control programs is made to memorize, when manufacturing equipment. Moreover, the 2nd approach is the approach of inputting from the actuation switch 8, and the 3rd approach is the approach of inputting from an external interface 7.

[0065] The 1st approach is divided, when making a key which is different in each of equipment memorize further, and when making the key common to a certain kind of all equipments memorize. However, it must apply so that only the person of normal using the equipment of the fake another place may know the decode key corresponding to an encryption key in the case of which, and difficulty may be actually accompanied by the employment.

[0066] Since the 2nd approach can carry out the direct input of the encryption key with which the user of equipment itself knows himself to equipment, there are few possibilities that other persons may get to know an encryption key, and it has the advantage whose safety improves rather than the 1st approach.

However, since the key which human being tends to treat cannot necessarily be defined freely, human being may memorize or, in the case of the key of magnitude or the contents difficult for inputting, the actuation may become with a troublesome thing.

[0067] The 3rd approach is the approach of connecting the suitable external device for an external interface 7, and inputting a cryptographic key into a picture input device from the external device. If the communication link for inputting a key is made to be performed with the question of an external device and a picture input device automatically when adopting this approach, human being's time and effort will be mitigated.

[0068] Next, the case where an IC card is adopted as an external device connected to an external interface 7 is explained. The user of a picture input device carries an IC card with a certain amount of anamnesis and count capacity, and presupposes into it that the encryption key which only the user knows, and a corresponding decode key are memorized.

[0069] It is thought that disassembling an IC card and obtaining the encryption key can be manufactured so that it may become very difficult. When a user uses a picture input device, its own IC card is connected to an external interface 7. It enciphers by the cryptographic key into which the photoed image is inputted from an IC card, and a picture input device is outputted and eliminates the

inputted encryption key after encryption termination.

[0070] When it does in this way, only the user with a corresponding decode key can decode the enciphered image information. Since a user connects his own IC card to an external interface and should just perform photography actuation at the time of actuation, there are few burdens on actuation than the 2nd approach.

[0071] They may be combined with the case where public key encryption or a common key encryptosystem is independently used as a cipher system. Even if it specifies an encryption key and enciphers by which approach, the cipher can be decoded using a corresponding decode key, and it is possible to obtain the image information by which information source coding was carried out.

[0072] As an example, the case where a common key encryptosystem is used independently is described. As shown in drawing 1 , IC card 20 is used as an external device. It is, when the means of communications for inputting an encryption key into said IC card 20 as the cryptographic key generation means of a common key encryptosystem at a picture input device is prepared.

[0073] An encryption key is generated by generating a random number, and makes the activation easy. A user connects IC card 20 to a picture input device through an external interface 7, and performs photography actuation. IC card 20 connected to the external interface 7 transmits the generated encryption key to a picture input device through means of communications.

[0074] A picture input device enciphers with the encryption vessel 5, and outputs the image photoed using the inputted encryption key. And after the encryption key used in order to generate this code completes encryption, it is eliminated from the memory of a picture input device. If a user connects IC card 20 to an information processor, an information processor can decode the image outputted from the picture input device using the encryption key read from IC card 20.

[0075] In addition, a scanner, a still camera, a video camera, etc. can be considered as a picture input device explained above. Otherwise, it is possible to apply this invention also to a copying machine or facsimile. Furthermore, it is clear that this invention is applicable about the information input unit of arbitration, such as a keyboard, a mouse, a pen tablet, a sensor, and a touch panel.

[0076] (Gestalt of the 2nd operation) Next, the case where public key encryption and a common key encryptosystem are combined as a cipher system is explained. Suppose that the encryption key generation means of public key encryption and means of communications with a picture input device are arranged by the IC card, using an IC card as an external device. The random-number-generation means, the public-key-encryption-ized means, and the common key encryptosystem-ized means shall be built in the picture input

device.

[0077] A user connects an IC card to a picture input device, and performs photography actuation. The connected IC card communicates the encryption key (below, it is called a public key) of public key encryption to a picture input device.

[0078] Using the generated encryption key, a picture input device enciphers with a built-in common key encryptosystem-ized means, and outputs the image which generated and photoed the encryption key for common-key-encryptosystem-izing using the random-number-generation means formed in the random number generator.

[0079] The encryption key for the common-key-encryptosystem-izing is enciphered and outputted to it and coincidence with a public-key-encryption-ized means using the public key into which it was inputted. The encryption key for common-key-encryptosystem-izing is eliminated from the memory of a picture input device after encryption termination.

[0080] A user connects an IC card to an information processor, decodes the encryption key for common-key-encryptosystem-izing enciphered with the public key encryption outputted from the picture input device with the private key corresponding to the public key in which it is stored by the IC card, and gets the encryption key used for common-key-encryptosystem-izing. And the encryption

image outputted from the picture input device is decoded using the encryption key.

[0081] Drawing 2 is a functional block diagram explaining each means constituted by the computer system which consists of the central information processor 2 of drawing 1 , memory 3 for control programs, and working-level month memory 4.

[0082] As shown in drawing 2 , the picture input device 100 of the gestalt of this operation has the image pick-up means 101, the conversion means 102, the coding means 103, the encryption means 104, the encryption key elimination means 105, means of communications 107, the record means 108, and the encryption key means forming 109.

[0083] Said image pick-up means 101 photos a photographic subject, and generates a picture signal, and the conversion means 102 is for changing said picture signal into digital information.

[0084] Moreover, the coding means 103 carries out high efficiency coding of said digital information, and the encryption means 104 is for enciphering said encoded digital information.

[0085] The encryption key means forming 109 is for inputting an encryption key for said encryption means enciphering from generating or the outside, and the encryption key elimination means 105 eliminates said encryption key, after said

encryption means completes encryption of digital information.

[0086] Means of communications 107 outputs said enciphered digital information outside, and the record means 108 records said enciphered digital information on a storage.

[0087] Next, the image input approach of the picture input device constituted as mentioned above is explained, referring to the flow chart of drawing 3 . As shown in drawing 3 , in the first step S1, the picture input device 100 of the gestalt of this operation photos a photographic subject with the image pick-up means 101, and generates a picture signal.

[0088] Next, it progresses to step S2 and the conversion means 102 performs transform processing which changes said picture signal into digital information. Then, it progresses to step S3 and high efficiency coding of said digital information is carried out with the coding means 103.

[0089] Next, it progresses to step S4 and encryption key formation processing in which the encryption key for enciphering said encoded digital information is inputted from generating or the outside by the encryption key means forming 109 is performed. Next, it progresses to step S5 and said encoded digital information is enciphered with the encryption means 104 using said encryption key.

[0090] Next, it progresses to step S6, and after completing encryption of said digital information, encryption key elimination processing which eliminates said

encryption key with the encryption key elimination means 105 is performed.

[0091] Since an encryption key is eliminated after encryption termination according to the image input approach of the gestalt this operation as explained above, it becomes impossible for a third person to get the encryption key (decode key) for decoding the enciphered information.

[0092] Therefore, in the case of the picture input device of the gestalt of this operation, safety can be maintained, without being dependent on the tamper resistance of an information input device. And it can respond now to many and unspecified users by inputting an encryption key (decode key) into an information input unit using an external interface 7.

[0093] Convenience and safety can be raised to coincidence, without being able to save the time and effort of actuation of human being, and being able to lessen by this, a possibility that an encryption key may be stolen by the third person, and increasing the amount of memory.

[0094] (Other operation gestalten of this invention) Even if it applies this invention to the system which consists of two or more devices (for example, a host computer, an interface device, a reader, a printer, etc.), it may be applied to the equipment which consists of one device.

[0095] Moreover, so that the function of the operation gestalt mentioned above may be realized and various kinds of devices may be operated As opposed to

the computer in the equipment connected with said various devices, or a system The program code of the software for realizing the function of said operation gestalt is supplied. What was carried out by operating said various devices according to the program stored in the computer (CPU or MPU) of the system or equipment is contained under the category of this invention.

[0096] Moreover, the function of the operation gestalt which the program code of said software itself mentioned above in this case will be realized, and the storage which stored the means for supplying that program code itself and its program code to a computer, for example, this program code, constitutes this invention. As a storage which memorizes this program code, a floppy disk, a hard disk, an optical disk, a magneto-optic disk, CD-ROM, a magnetic tape, the memory card of a non-volatile, ROM, etc. can be used, for example.

[0097] Moreover, by performing the program code with which the computer was supplied, also when [, such as OS (operating system) or other application software with which the function of the above-mentioned operation gestalt is not only realized, but the program code is working in a computer,] the function of the above-mentioned operation gestalt is realized jointly, it cannot be overemphasized that this program code is contained in the operation gestalt of this invention.

[0098] Furthermore, after stored in the memory with which the functional

expansion unit by which the supplied program code was connected to the functional add-in board and the computer of a computer is equipped, also when the function of the operation gestalt which performed a part or all of processing that CPU with which the functional add-in board and functional expansion unit are equipped based on directions of the program code is actual, and mentioned above by the processing is realized, it cannot be overemphasized that it is contained in this invention.

[0099]

[Effect of the Invention] Since the encryption key was eliminated from the information input unit after encryption termination according to invention of this application as explained above, it can avoid obtaining a third person in the encryption key (decode key) for decoding the enciphered information. Thereby, high safety can be maintained, without being dependent on the tamper resistance of an information input device.

[0100] Moreover, convenience and safety can be raised to coincidence, without according to other descriptions of this invention, being able to respond to many and unspecified users, being able to save the time and effort of actuation of human being, and being able to lessen a possibility that an encryption key may be stolen by the third person, and increasing the amount of memory, since the encryption key (decode key) was inputted into the information input unit using

the interface with the exterior.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of the picture input device with an encryption function concerning the gestalt of operation of this invention.

[Drawing 2] It is the functional block diagram showing the functional configuration of the picture input device with an encryption function concerning the gestalt of operation of this invention.

[Drawing 3] It is the flow chart which shows an example of the image input approach of this invention.

[Description of Notations]

1 Image Pick-up Equipment

2 CPU

3 Memory for Control Programs

4 Working-level Month Memory

5 Encryption Machine

6 Mechanical Movement Section

7 External Interface

8 Actuation Switch

100 Picture Input Device

101 Image Pick-up Means

102 Conversion Means

103 Coding Means

104 Encryption Means

105 Encryption Key Elimination Means

107 Means of Communications

108 Record Means

109 Encryption Key Means Forming

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－205738

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ　5/92		Ｈ０４Ｎ	5/92	Ｚ
Ｈ０４Ｌ　9/10			5/907	Ｂ
Ｈ０４Ｎ　5/907		Ｈ０４Ｌ	9/00	６２１Ａ

審査請求　未請求　請求項の数21　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－3367

(22)出願日　平成10年(1998)１月９日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　大石　和臣
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

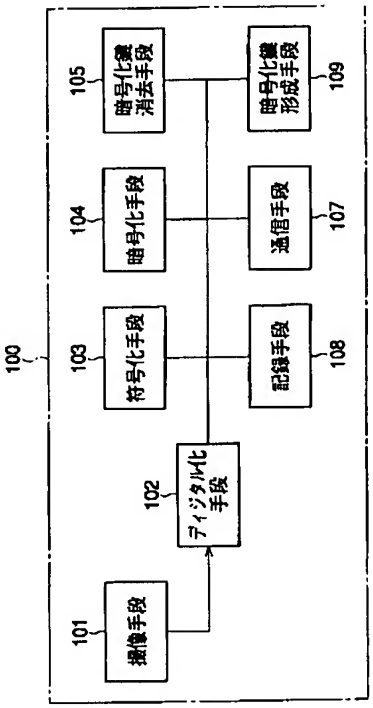
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　画像入力装置および方法並びに記憶媒体

(57)【要約】

【課題】　情報入力装置のタンパー・レジスタンスに依存することなく高い安全性を保つことができるようにする。

【解決手段】　画像信号をディジタル情報に変換する変換手段１０２と、前記ディジタル情報を暗号化する暗号化手段１０４と、前記暗号化手段１０４が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段１０９と、前記暗号化手段１０４がディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去手段１０５とを設け、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得られないようにする。



【特許請求の範囲】
【請求項１】　画像信号をディジタル情報に変換する変換手段と、
暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化手段と、
前記暗号化手段が前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去手段とを有することを特徴とする画像入力装置。
【請求項２】　前記変換手段は前記ディジタル情報を高能率符号化する符号化手段を有し、前記暗号化手段は前記高能率符号化したディジタル情報を暗号化することを特徴とする請求項１に記載の画像入力装置。
【請求項３】　被写体を撮影して画像信号を生成する撮像手段を有し、前記変換手段は前記撮像手段により生成された画像信号をディジタル情報に変換することを特徴とする請求項１または２に記載の画像入力装置。
【請求項４】　前記暗号化鍵を外部から入力する暗号化鍵入力手段を具備することを特徴とする請求項１～３の何れか１項に記載の画像入力装置。
【請求項５】　前記暗号化鍵を内部で発生する暗号化鍵発生手段を具備することを特徴とする請求項１～３の何れか１項に記載の画像入力装置。
【請求項６】　前記暗号化鍵は共通鍵暗号化のための暗号化鍵であることを特徴とする請求項４または５に記載の画像入力装置。
【請求項７】　前記暗号化鍵発生手段で発生された内部暗号化鍵を外部から入力するインターフェースを具備し、前記インターフェースを介して暗号化された内部暗号化鍵を出力することを特徴とする請求項５に記載の画像入力装置。
【請求項８】　前記内部暗号化鍵は共通鍵暗号化のための暗号化鍵であり、前記外部暗号化鍵は公開鍵暗号化のための暗号化鍵であることを特徴とする請求項７に記載の画像入力装置。
【請求項９】　前記暗号化したディジタル情報を外部に出力する通信手段を具備することを特徴とする請求項１～８の何れか１項に記載の画像入力装置。
【請求項１０】　前記暗号化したディジタル情報を記録する記録手段を具備することを特徴とする請求項１～９の何れか１項に記載の画像入力装置。
【請求項１１】　画像信号をディジタル情報に変換する変換処理と、
暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化処理と、
前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去処理とを行うことを特徴とする画像入力方法。
【請求項１２】　前記ディジタル情報を高能率符号化し、前記高能率符号化されたディジタル情報を暗号化することを特徴とする請求項１１に記載の画像入力方法。
【請求項１３】　被写体を撮影する撮像処理により前記画像信号を生成することを特徴とする請求項１１または１２に記載の画像入力方法。
【請求項１４】　前記暗号化したディジタル情報を外部に出力する出力処理を行うことを特徴とする請求項１１～１３の何れか１項に記載の画像入力方法。
【請求項１５】　前記暗号化したディジタル情報を記録する記録処理を行うことを特徴とする請求項１１～１４の何れか１項に記載の画像入力方法。
【請求項１６】　請求項１～１０に記載の各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴とする記憶媒体。
【請求項１７】　請求項１１～１５の何れか１項に記載の画像入力方法の手順をコンピュータに実行させるためのプログラムを格納したことを特徴とする記憶媒体。
【請求項１８】　画像信号をディジタル情報に変換する変換手段と、
前記ディジタル情報を暗号化する暗号化手段と、
前記暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴とする画像入力装置。
【請求項１９】　画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を暗号化する暗号化手段とを有する画像入力装置に対して着脱自在であり、
前記暗号化手段が暗号化を行うため、および暗号化された前記ディジタル情報を復号するための鍵を記憶することを特徴とする記憶媒体。
【請求項２０】　画像信号をディジタル情報に変換する変換手段と、
前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、
前記内部暗号化鍵を暗号化する鍵暗号化手段と、
前記鍵暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴とする画像入力装置。
【請求項２１】　画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、前記内部暗号化鍵を暗号化する鍵暗号化手段とを有する画像入力装置に対して着脱自在であり、
前記鍵暗号化手段が暗号化を行うための暗号化鍵および暗号化された前記内部暗号化鍵を復号するための復号鍵を記憶することを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、画像入力装置および方法並びに記憶媒体に関するものである。
【０００２】
【従来の技術】スチル・カメラやビデオ・カメラ、あるいはスキャナ等のような画像入力装置は、被写体を撮影

して得られた画像信号や、動画像や静止画像等の画像信号を入力し、画像情報として再生できるような形式に変換して出力したり、あるいは記録装置を用いて記憶媒体に記録したりするようにしている。

【０００３】前記記憶媒体は、ある程度の長期間にわたって保存することが可能であるので、前記保存した画像情報を後で観賞したり、あるいは再利用したりするのに都合が良い。また、再生装置は、前記記憶媒体に記録された画像情報から人間にとって有意義な画像を形成し、プリンターやディスプレイ等の出力装置を用いて画像を再現する。

【０００４】最近は、ディジタル技術の進展により、従来はアナログ方式で実現されていた前記画像入力装置等は、ディジタル方式のものに徐々に切り換えられつつある。これらのディジタル方式の画像入力装置は、ほとんどの場合、撮影対象あるいは入力対象を光学的に捉え、それを光電変換して電気信号を生成し、次いでアナログ／ディジタル変換した後、所定の画像処理を施すようにしている。そして、その結果として形成される画像／画像情報を予め定められた形式のディジタル情報として出力する。

【０００５】ここで、予め定められた形式とは、ＭＨ、ＭＲ、ＭＭＲ、ＴＩＦＦ、ＪＰＥＧ、ＭＰＥＧ等といった画像／画像情報に対する情報源符号化方式による符号のことを意味している。

【０００６】そして、再生装置がその復号アルゴリズムを用いることにより、符号から復号して形成した情報をプリンターやディスプレイ等の出力装置に出力したときに、人間が画像／画像として理解できるような情報である。

【０００７】以下では、前述の予め定められた形式のディジタル情報として出力される画像／画像情報を、情報源符号化された画像／画像情報と呼ぶ。情報源符号化された画像／画像情報、あるいはそれから復号された画像／画像情報を、例えばパーソナル・コンピュータのような情報処理装置に取り込み、その形式に対応した画像／画像情報編集処理ソフトウェアを用いて編集することは極めて容易である。

【０００８】情報源符号化された画像／画像情報、あるいはそれを編集した情報を複製したときの画質は原本と全く同一である。従来のアナログ方式の場合には、編集や複製は画質の劣化を必ずもたらしていたために画像処理に制限が課されていたが、この点でディジタル方式は圧倒的な利便性の向上をもたらした。

【０００９】ところで、従来のアナログ方式では複製を繰り返すことは必ず画質の劣化を伴ったがゆえに、違法な複製行為が行なわれるということはあってもそれが現実的に大きな問題となることは少なかった。したがって、そのような不正な複製行為を禁止する方法は特に設けられていなかった。

【００１０】しかし、ディジタル方式では原本と全く同一の複製を無制限に生成することが可能であるので、複製行為を誰でも自由に行なえるとすれば、著作物の観賞権利に対する対価を消費者が映画等の画像著作物の製作者等に対して払う必要は無くなるので、著作物の製作者等に対して大きな脅威となることは明らかである。

【００１１】あるいは別の例として、例えば、著作物の原本となる画像／画像情報が情報源符号化された画像情報としてコンピュータに記録されている場合に、クラッカーがそのコンピュータにアクセスし、その画像／画像情報を不当に複製して、正規の著作物製品よりも安い価格で販売することや、その著作物を新たに編集して他の著作物として販売することも考えられる。

【００１２】以上のような、ディジタル情報の複製の問題に対して、次に述べる暗号の技術を用いた対策が有効である。なお、暗号とは、情報の意味が当時者以外にはわからないように情報を変換することをいう。

【００１３】暗号において、元の文を平文という。また、それを第三者には意味が分からない暗号文に変えることを暗号化といい、その変換手順を暗号アルゴリズムという。平文、暗号文といってもテキストに限るわけではなく、データ、音声、画像などあらゆる情報を想定している。

【００１４】暗号化は、暗号化鍵というパラメータに依存する変換である。当事者が暗号文を元の平文に戻すことを復号といい、暗号化鍵に対応するパラメータ（復号鍵と呼ぶ）を用いて行なう。

【００１５】また、当事者以外の第三者が暗号文を元の平文に戻すこと、あるいは復号鍵を見いだすことを解読という。現代の暗号では、暗号の安全性を暗号あるいは復号に用いる鍵に帰着させており、鍵を知らなければたとえ暗号アルゴリズムを知っていても平文は得られないように作られている。したがって、暗号器の作成者でも解読はできない。

【００１６】暗号には多くのアルゴリズムがあるが、以下では暗号化鍵を公開できるか否かの観点から、非対称暗号（公開鍵暗号）と対称暗号（慣用暗号）の二つに分類する。

【００１７】非対称暗号は公開鍵暗号とも呼ばれ、暗号化鍵と復号鍵が異なり、暗号化鍵から復号鍵が容易に計算できないようになっており、暗号化鍵を公開鍵といい、復号鍵を秘密に保持して使われる暗号のことをいう。

【００１８】非対称暗号は、以下の特徴を持っている。

（１）暗号化鍵と復号鍵とが異なり暗号化鍵を公開できるため、暗号化鍵を秘密に配送する必要がなく、鍵配送が容易である。

（２）各利用者の暗号化鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（３）送られてきた通信文の送信者が偽物でないこと、

及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。暗号機能と認証機能を実現できる非対称暗号として、ＲＳＡ暗号（R. L. Rivest, A. Shamir and L. Adleman, “A method ofobtaining digital signatures and public key cryptosytems,” Comm of ACM, ）がある。

【００１９】また、この他に、エルガマル暗号（T. E. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transaction on Information Theory, Vol. IT-31, No. 4, pp-469－472, １９８５）が有名である。

【００２０】認証機能のみを実現できる非対称暗号として、Ｆｉａｔ-Ｓｈａｍｉｒ暗号（A. Fiat, A. Shamir, “How to prove yourself:practical solutions of idcntification and signature problems,”, Proc. of CRYPTO’８６, １９８７）や、Ｓｃｈｎｏｒｒ暗号（C. P. Schnorr, “Emcient signature generationby smart cards,” Journal of Cryptolgyvol 4, pp. １６１－１７４, １９９１）が有名である。

【００２１】対称暗号は、暗号化鍵と復号鍵が同一の暗号であり、共通鍵暗号とも呼ばれている。１９７９年代後半に公開鍵暗号が現れて、従来から存在する対称暗号は慣用暗号とも呼ばれるようになった。

【００２２】対称暗号は、適当な長さの文字列（ブロック）ごとに同じ鍵で暗号化するブロック暗号と、文字列またはビットごとに鍵を変えていくストリーム暗号に分けることができる。

【００２３】ブロック暗号には、文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に換える換字式暗号等があり、アルゴリズムが公開されているＤＥＳ（Data Encryption Standard）や、ＦＥＡＬ（Fastdata Encipherment ALgorithm）といった暗号が商用暗号として広く用いられている。

【００２４】ストリーム暗号は、メッセージに乱数をＸＯＲ（排他論理和）して、内容を撹乱する方式であり、無限周期の乱数列を１回限りの使い捨て鍵として用いるバーナム暗号が有名である。

【００２５】以上の暗号の技術を用いて、コンピュータ等に記録される画像／画像情報等に対して暗号化を施し、復号鍵を安全に保管しておけば、暗号文、つまり画像／画像情報を暗号化した情報が盗まれて複製されたとしても、画像／画像情報そのものが盗まれたことにはならないので被害を被ることはない。つまり、前述のような複製の問題を解決できると考えられる。

【００２６】ところが、従来は画像／画像情報等がコンピュータ等に出力されてからコンピュータ上で暗号化が実行されていたので、画像入力装置から画像／画像情報が出力されてからコンピュータ上で暗号化されるまでの間は情報源符号化された画像／画像情報として存在し、その間に画像／画像情報を盗まれてしまうという問題があった。

【００２７】この問題に対して、画像入力装置内部で暗号化を行なう対処法がある。このとき、暗号化される前の画像／画像情報が外部に取り出されることが無いように暗号化機能を組み込む必要がある。

【００２８】このような手段としては、その内部に格納してあるプログラムやデータを取り出すことが物理的に困難になるように暗号化部をＩＣチップ化することや、さらには、ＩＣチップ化した暗号化部の内部にセンサーを設けておき、ＩＣチップ内部のデータを取り出そうとする物理的動作を検出したときにその内部のプログラムやデータを消去・破壊するといったものが考えられる。このような外部からの攻撃に対する耐性をタンパー・レジスタンス（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ）と呼ぶ。

【００２９】

【発明が解決しようとする課題】タンパー・レジスタンスを有する暗号化部を組み込んだ画像入力装置では、その強度を弱めないために、固定の値が暗号化鍵としてあらかじめ装置に記録されており、その値は容易に変更できないことが普通である。

【００３０】一つの装置に一つの鍵が割り当てられている場合、複数のユーザがそれを共有して使う時にはそれらのユーザー間では暗号化（秘匿）機能は無いに等しいことになってしまう。

【００３１】一方、複数の鍵をあらかじめ用意しておき、ユーザ毎に別々の鍵を用いるという方法もあるが、この時は装置内部の暗号化部のメモリ量が増え、コストの上昇につながる問題が生じる。

【００３２】いずれにせよ、不特定多数のユーザに対して個別に対応できないという問題があった。さらに、これらのタンパー・レジスタンスを有する装置や媒体は、その性質を永遠に有するとは限らず、新しい攻撃手段によりその性質が容易に無効化される恐れもあった。

【００３３】本発明は前述の問題点にかんがみ、情報入力装置のタンパー・レジスタンスに依存することなく安全性を保つことができるようにすることを目的とする。

【００３４】

【課題を解決するための手段】本発明の画像入力装置は、画像信号をディジタル情報に変換する変換手段と、

暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化手段と、前記暗号化手段が前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去手段とを有することを特徴としている。

【００３５】また、本発明の画像入力装置の他の特徴とするところは、前記変換手段は前記ディジタル情報を高能率符号化する符号化手段を有し、前記暗号化手段は前記高能率符号化したディジタル情報を暗号化することを特徴としている。

【００３６】また、本発明の画像入力装置のその他の特徴とするところは、被写体を撮影して画像信号を生成する撮像手段を有し、前記変換手段は前記撮像手段により生成された画像信号をディジタル情報に変換することを特徴としている。

【００３７】また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵を外部から入力する暗号化鍵入力手段を具備することを特徴としている。

【００３８】また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵を内部で発生する暗号化鍵発生手段を具備することを特徴としている。

【００３９】また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵は共通鍵暗号化のための暗号化鍵であることを特徴としている。

【００４０】また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵発生手段で発生された内部暗号化鍵を外部から入力するインターフェースを具備し、前記インターフェースを介して暗号化された内部暗号化鍵を出力することを特徴としている。

【００４１】また、本発明の画像入力装置のその他の特徴とするところは、前記内部暗号化鍵は共通鍵暗号化のための暗号化鍵であり、前記外部暗号化鍵は公開鍵暗号化のための暗号化鍵であることを特徴としている。

【００４２】また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化したディジタル情報を外部に出力する通信手段を具備することを特徴としている。

【００４３】また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化したディジタル情報を記録する記録手段を具備することを特徴としている。

【００４４】本発明の画像入力方法は、画像信号をディジタル情報に変換する変換処理と、暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化処理と、前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去処理とを行うことを特徴としている。

【００４５】また、本発明の画像入力方法の他の特徴とするところは、前記ディジタル情報を高能率符号化し、前記高能率符号化されたディジタル情報を暗号化することを特徴としている。

【００４６】また、本発明の画像入力方法のその他の特徴とするところは、被写体を撮影する撮像処理により前記画像信号を生成することを特徴としている。

【００４７】また、本発明の画像入力方法のその他の特徴とするところは、前記暗号化したディジタル情報を外部に出力する出力処理を行うことを特徴としている。

【００４８】また、本発明の画像入力方法のその他の特徴とするところは、前記暗号化したディジタル情報を記録する記録処理を行うことを特徴としている。

【００４９】また、本発明の記憶媒体は、前記各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴としている。

【００５０】また、本発明の記憶媒体の他の特徴とするところは、前記画像入力方法の手順をコンピュータに実行させるためのプログラムを格納したことを特徴としている。

【００５１】また、本発明の画像入力装置のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を暗号化する暗号化手段と、前記暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴としている。

【００５２】また、本発明の記憶媒体のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を暗号化する暗号化手段とを有する画像入力装置に対して着脱自在であり、前記暗号化手段が暗号化を行うため、および暗号化された前記ディジタル情報を復号するための鍵を記憶することを特徴としている。

【００５３】また、本発明の画像入力装置のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、前記内部暗号化鍵を暗号化する鍵暗号化手段と、前記鍵暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴としている。

【００５４】また、本発明の記憶媒体のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、前記内部暗号化鍵を暗号化する鍵暗号化手段とを有する画像入力装置に対して着脱自在であり、前記鍵暗号化手段が暗号化を行うための暗号化鍵および暗号化された前記内部暗号化鍵を復号するための復号鍵を記憶することを特徴としている。

【００５５】本発明は前記技術手段よりなるので、暗号化鍵は暗号化終了後には情報入力装置から消去され、これにより、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得ることができなくなり、情報入力装置のタンパー・レジスタンスに依存することなく安全性を保つことが可能となる。

【００５６】また、本発明の他の特徴によれば、外部とのインターフェイスを利用して暗号化鍵（復号鍵）を入

力するので、不特定多数のユーザに対応することができ、人間の操作の手間を省くことができるようになるとともに、暗号化鍵が第三者に盗まれる恐れを少なくすることができるようになる。

【００５７】

【発明の実施の形態】（第１の実施の形態）次に、図１を参考に本発明の画像入力装置および方法並びに記憶媒体の第１の実施の形態を説明する。

【００５８】図１は、本実施の形態の画像入力装置の概略を示すブロック図であり、１は撮像装置、２は中央情報処理装置（ＣＰＵ）、３は制御プログラム用メモリ、４は作業用メモリ、５は暗号化器であり、これはタンパー・レジスタンスを持つように封止一体化されたモジュール１０となっていることを示している。

【００５９】本実施の形態の画像入力装置においては、読みとる対象を撮像装置１により撮像してアナログの画像信号を生成し、これをディジタル画像信号に変換するディジタル変換処理を施すようにしている。

【００６０】前記撮像装置１は、制御プログラム用メモリ３に格納されているプログラムによって良い画像が得られるように制御され、その結果として画像データを出力するように動作する。

【００６１】次に、この画像データは、ＣＰＵ２において画像処理等を施された後、情報源符号化（高能率符号化）された画像／画像情報に変換されて、暗号化器５に入力される。暗号化器５は、外部インターフェイス７から入力される暗号化鍵をパラメータとして、入力に対する暗号化をその内部で実行して暗号文を生成して出力する。出力された暗号化された画像データは不図示の記憶媒体に記憶される。外部インターフェイス７は、暗号化鍵を装置外部から受け取ったり、あるいは装置内から暗号化鍵を出力するために使われたりするインターフェイスである。

【００６２】前記の構成において、タンパー・レジスタンスの特徴により、撮像装置１と、ＣＰＵ２と、制御プログラム用メモリ３と、作業用メモリ４と、暗号化器５の内部に存在するデータや通信内容を外部から得ることはできない。

【００６３】次に、暗号化に用いる暗号方式、暗号化鍵の指定方法の組合せについて説明する。用いる暗号方式は、公開鍵暗号と共通鍵暗号の２つの場合がある。共通鍵暗号を用いる場合は、暗号化鍵を他者に知られないように指定する必要がある。これに対して公開鍵暗号を用いる場合は、暗号化鍵は公開可能であるので必ずしも他者に知られないように指定する必要はない。

【００６４】暗号化鍵の指定方法は、以下のような方法がある。すなわち、第１の方法は装置を製造する時に制御プログラム用メモリ３に記憶させておく方法である。また、第２の方法は、操作スイッチ８から入力する方法であり、第３の方法は、外部インターフェイス７から入力する方法である。

【００６５】第１の方法は、さらに、装置の一つ一つに異なった鍵を記憶させておく場合と、ある種類の装置の全てに共通の鍵を記憶させておく場合とに分けられる。しかし、いずれの場合にせよその装置を使う正規の者だけが暗号化鍵に対応する復号鍵を知るように運用しなければならず、その運用は現実的には困難が伴うことがある。

【００６６】第２の方法は、装置の使用者自身が自分しか知らない暗号化鍵を装置に直接入力できるので、他の者が暗号化鍵を知る恐れは少なく、第１の方法よりも安全性が向上する利点を有している。しかし、人間が扱いやすい鍵を自由に定められるとは限らないので、人間が記憶したり入力するのに困難な大きさや内容の鍵の場合には、その操作は煩わしいものとなることがある。

【００６７】第３の方法は、外部インターフェイス７に適当な外部装置を接続して、その外部装置から画像入力装置に暗号鍵を入力する方法である。この方法を採用する場合、鍵を入力するための通信が外部装置と画像入力装置との間で自動的に行なわれるようにすれば、人間の手間は軽減される。

【００６８】次に、外部インターフェイス７に接続される外部装置としてＩＣカードを採用した場合について説明する。画像入力装置のユーザは、ある程度の記憶能力と計算能力を持つＩＣカードを携帯し、その中にはそのユーザだけが知っている暗号化鍵と対応する復号鍵が記憶されるとする。

【００６９】ＩＣカードを分解してその暗号化鍵を得ることは極めて困難になるように製造できると考えられる。ユーザが画像入力装置を使用する時に、自分のＩＣカードを外部インターフェイス７に接続する。画像入力装置は、撮影した画像をＩＣカードから入力される暗号鍵で暗号化して出力し、入力された暗号化鍵を暗号化終了後に消去する。

【００７０】このようにすると、暗号化された画像情報は、対応する復号鍵を持つそのユーザだけが復号できることになる。ユーザは、操作時に自分のＩＣカードを外部インターフェイスに接続して撮影操作を行なうだけでよいので、操作上の負担は第２の方法よりは少ない。

【００７１】暗号化方式として公開鍵暗号あるいは共通鍵暗号を単独に利用する場合と、それらを組み合わせる場合がある。いずれの方法で暗号化鍵を指定して暗号化したとしても、その暗号文は対応する復号鍵を用いて復号することができ、情報源符号化された画像情報を得ることが可能である。

【００７２】一例として、共通鍵暗号を単独に用いる場合について述べる。図１に示したように、外部装置としてＩＣカード２０を用いる。前記ＩＣカード２０には共通鍵暗号の暗号鍵生成手段と、暗号化鍵を画像入力装置に入力するための通信手段が設けられているという。

【００７３】暗号化鍵は、例えば、乱数を発生させることにより生成され、その実行は容易であるものとする。ユーザがＩＣカード２０を外部インターフェイス７を介して画像入力装置に接続し、撮影操作を行なう。外部インターフェイス７に接続されたＩＣカード２０は、通信手段を介して、生成した暗号化鍵を画像入力装置に送信する。

【００７４】画像入力装置は、入力された暗号化鍵を用いて撮影した画像を暗号化器５により暗号化して出力する。そして、この暗号を生成するために用いられた暗号化鍵は、暗号化を終了した後で画像入力装置のメモリから消去される。ユーザはＩＣカード２０を情報処理装置に接続すると、情報処理装置はＩＣカード２０から読みだした暗号化鍵を用いて、画像入力装置から出力された画像を復号することができる。

【００７５】なお、以上に説明した画像入力装置としては、スキャナやスチル・カメラ、ビデオ・カメラ等が考えられる。他に、複写機やファクシミリにも本発明を適用することが可能である。さらに、キーボード、マウス、ペン・タブレット、センサー、タッチ・パネル等のような、任意の情報入力装置に関して、本発明を適用できることは明らかである。

【００７６】（第２の実施の形態）次に、暗号化方式として公開鍵暗号と共通鍵暗号を組み合わせる場合について説明する。外部装置としてＩＣカードを用い、ＩＣカードには公開鍵暗号の暗号化鍵生成手段と、画像入力装置との通信手段が配設されているとする。画像入力装置には、乱数発生手段と公開鍵暗号化手段と共通鍵暗号化手段が内蔵されているものとする。

【００７７】ユーザがＩＣカードを画像入力装置に接続し、撮影操作を行なう。接続されたＩＣカードは公開鍵暗号の暗号化鍵（以下では、公開鍵と呼ぶ）を画像入力装置に通信する。

【００７８】画像入力装置は、乱数発生器に設けられている乱数発生手段を用いて共通鍵暗号化のための暗号化鍵を生成し、撮影した画像をその生成した暗号化鍵を用いて内蔵の共通鍵暗号化手段により暗号化して出力する。

【００７９】それと同時に、その共通鍵暗号化のための暗号化鍵を、入力された公開鍵を用いて公開鍵暗号化手段で暗号化して出力する。共通鍵暗号化のための暗号化鍵は暗号化終了後に画像入力装置のメモリから消去される。

【００８０】ユーザはＩＣカードを情報処理装置に接続し、画像入力装置から出力された公開鍵暗号で暗号化された共通鍵暗号化のための暗号化鍵を、ＩＣカードに格納されている公開鍵に対応する秘密鍵で復号し、共通鍵暗号化のために使われた暗号化鍵を得る。そして、その暗号化鍵を用いて、画像入力装置から出力された暗号化画像を復号する。

【００８１】図２は、図１の中央情報処理装置２、制御プログラム用メモリ３、作業用メモリ４からなるコンピュータシステムにより構成される各手段を説明する機能ブロック図である。

【００８２】図２に示したように、本実施の形態の画像入力装置１００は、撮像手段１０１と、変換手段１０２と、符号化手段１０３と、暗号化手段１０４と、暗号化鍵消去手段１０５と、通信手段１０７と、記録手段１０８と、暗号化鍵形成手段１０９とを有している。

【００８３】前記撮像手段１０１は、被写体を撮影して画像信号を生成するものであり、変換手段１０２は、前記画像信号をディジタル情報に変換するためのものである。

【００８４】また、符号化手段１０３は、前記ディジタル情報を高能率符号化するものであり、暗号化手段１０４は前記符号化したディジタル情報を暗号化するためのものである。

【００８５】暗号化鍵形成手段１０９は、前記暗号化手段が暗号化を行うための暗号化鍵を発生もしくは外部から入力するためのものであり、暗号化鍵消去手段１０５は前記暗号化手段がディジタル情報の暗号化を終了した後に前記暗号化鍵を消去するものである。

【００８６】通信手段１０７は、前記暗号化したディジタル情報を外部に出力するものであり、記録手段１０８は前記暗号化したディジタル情報を記憶媒体に記録するものである。

【００８７】次に、前述のように構成された画像入力装置の画像入力方法を図３のフローチャートを参照しながら説明する。図３に示したように、本実施の形態の画像入力装置１００は、最初のステップＳ１において、被写体を撮像手段１０１で撮影して画像信号を生成する。

【００８８】次に、ステップＳ２に進み、前記画像信号をディジタル情報に変換する変換処理を変換手段１０２により行う。その後、ステップＳ３に進み、符号化手段１０３によって前記ディジタル情報を高能率符号化する。

【００８９】次に、ステップＳ４に進み、前記符号化されたディジタル情報を暗号化するための暗号化鍵を暗号化鍵形成手段１０９にて発生もしくは外部から入力する暗号化鍵形成処理を行う。次に、ステップＳ５に進み、前記符号化されたディジタル情報を前記暗号化鍵を用いて暗号化手段１０４で暗号化する。

【００９０】次に、ステップＳ６に進み、前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を暗号化鍵消去手段１０５によって消去する暗号化鍵消去処理を行う。

【００９１】以上説明したように、本実施の形態の画像入力方法によれば、暗号化鍵は暗号化終了後には消去されるので、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得ることができなくなる。

【００９２】したがって、本実施の形態の画像入力装置の場合には、情報入力装置のタンパー・レジスタンスに依存することなく安全性を保つことができる。しかも、外部インターフェイス７を利用して暗号化鍵（復号鍵）を情報入力装置に入力することにより、不特定多数のユーザに対応することができるようになる。

【００９３】これにより、人間の操作の手間を省き、暗号化鍵を第三者に盗まれる恐れを少なくすることができ、かつメモリ量を増やすこと無しに、利便性と安全性を同時に向上させることができる。

【００９４】（本発明の他の実施形態）本発明は複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【００９５】また、前述した実施形態の機能を実現するように各種のデバイスを動作させるように、前記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、前記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００９６】また、この場合、前記ソフトウェアのプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００９７】また、コンピュータが供給されたプログラムコードを実行することにより、前述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して前述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【００９８】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【００９９】

【発明の効果】以上説明したように、本出願の発明によれば、暗号化終了後には情報入力装置から暗号化鍵を消去するようにしたので、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得られないようにすることができる。これにより、情報入力装置のタンパー・レジスタンスに依存することなく高い安全性を保つことができる。

【０１００】また、本発明の他の特徴によれば、外部とのインターフェイスを利用して暗号化鍵（復号鍵）を情報入力装置に入力するようにしたので、不特定多数のユーザに対応することができ、人間の操作の手間を省き、暗号化鍵を第三者に盗まれる恐れを少なくすることができ、かつメモリ量を増やすこと無しに、利便性と安全性を同時に向上させることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る暗号化機能付き画像入力装置の構成を示すブロック図である。

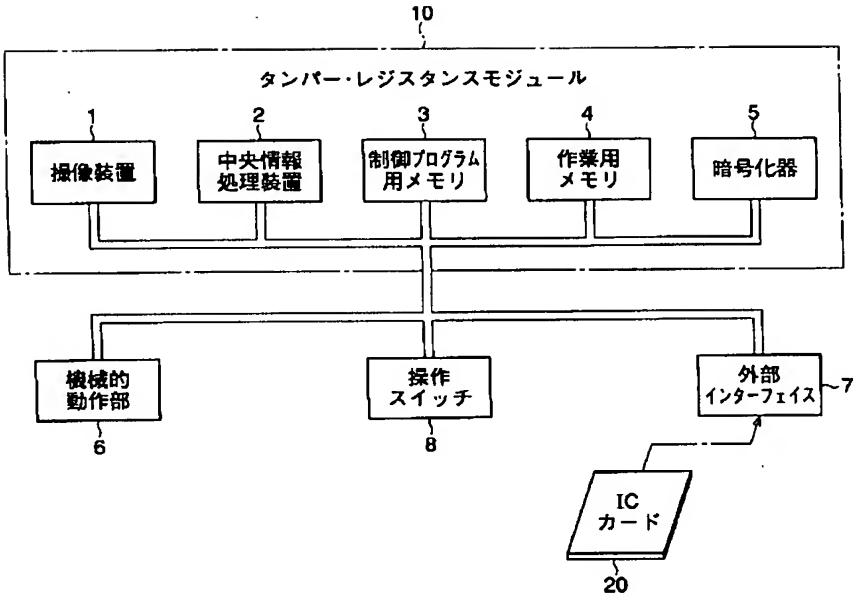
【図２】本発明の実施の形態に係る暗号化機能付き画像入力装置の機能構成を示す機能ブロック図である。

【図３】本発明の画像入力方法の一例を示すフローチャートである。

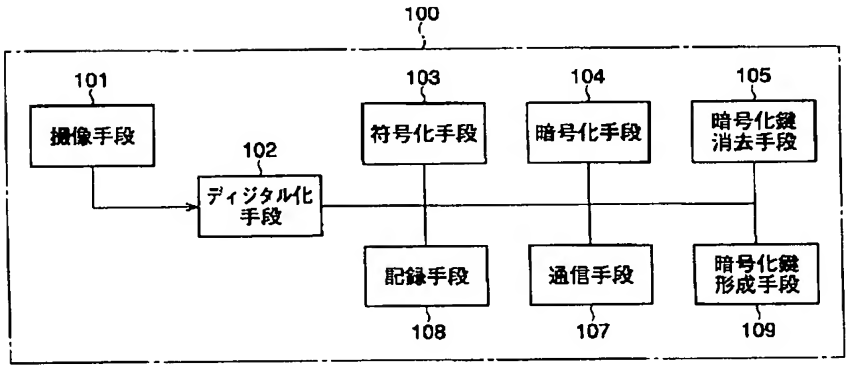
【符号の説明】

１　撮像装置
２　ＣＰＵ
３　制御プログラム用メモリ
４　作業用メモリ
５　暗号化器
６　機械的動作部
７　外部インターフェイス
８　操作スイッチ
１００　画像入力装置
１０１　撮像手段
１０２　変換手段
１０３　符号化手段
１０４　暗号化手段
１０５　暗号化鍵消去手段
１０７　通信手段
１０８　記録手段
１０９　暗号化鍵形成手段

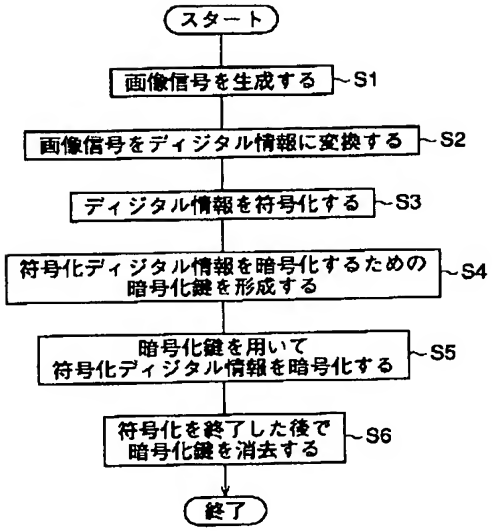
【図１】


10
タンパー・レジスタンスモジュール
1
撮像装置
2
中央情報処理装置
3
制御プログラム用メモリ
4
作業用メモリ
5
暗号化器
機械的動作部
6
操作スイッチ
8
外部インターフェイス
7
IC カード
20

【図２】


100
101
撮像手段
102
ディジタル化手段
103
符号化手段
104
暗号化手段
105
暗号化鍵消去手段
記録手段
108
通信手段
107
暗号化鍵形成手段
109

【図３】


スタート
画像信号を生成する
S1
画像信号をディジタル情報に変換する
S2
ディジタル情報を符号化する
S3
符号化ディジタル情報を暗号化するための暗号化鍵を形成する
S4
暗号化鍵を用いて符号化ディジタル情報を暗号化する
S5
符号化を終了した後で暗号化鍵を消去する
S6
終了